Fortinet - FortiAnalyzer NSE5 Analyst

Durée: 1 Jour **Réf de cours: NSE5-AN** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

Dans ce cours, vous apprendrez les principes fondamentaux de l'utilisation de FortiAnalyzer pour la journalisation centralisée. Vous apprendrez également à identifier les menaces actuelles et potentielles grâce à l'analyse des journaux. Enfin, vous examinerez la gestion des événements, des incidents, des rapports et l'automatisation des tâches avec les playbooks.
Ces compétences vous fourniront une base solide pour devenir un analyste SOC dans un environnement utilisant les produits Fortinet. FortiAnalyzer est au cœur de la Security Fabric de Fortinet, offrant une journalisation et une analyse centralisées pour une visibilité complète. Cela permet aux analystes de gérer plus efficacement la posture de sécurité, d'automatiser les processus de sécurité et de répondre rapidement aux menaces.
Mis à jour 29/01/2025

Formation intra-entreprise

Cette formation est délivrable en session intra-entreprise, dans vos locaux ou dans les nôtres. Son contenu peut être adapté sur-mesure pour répondre aux besoins de vos collaborateurs. Contactez votre conseiller formation Global Knowledge ou adressez votre demande à info@globalknowledge.fr.

Public visé:

Cette formation est à destination d'ingénieurs techniques souhaitant utiliser FortiAnalyser en tant qu'analystes, responsables de l'analyse de la Security Fabric de Fortinet et de l'automatisation des tâches de détection et de réponse aux cyberattaques.

Objectifs pédagogiques:

- A l'issue de cette formation, les participants seront en mesure de :
- Comprendre les concepts et les fonctionnalités de base du FortiAnalyzer
- Décrire l'objectif de la collecte et du stockage des logs
- Visualiser et rechercher des logs dans Log View et FortiView
- Comprendre les fonctionnalités du SOC
- Gérer les événements et les gestionnaires d'événements
- Configurer et analyser les incidents
- Effectuer des tâches de détection des menaces
- Comprendre les alertes épidémiques
- Décrire le fonctionnement des rapports dans ADOM
- Personnaliser et créer des graphiques et des ensembles de données
- Personnaliser et exécuter des rapports
- Configurer le stockage externe pour les rapports
- Joindre des rapports aux incidents
- Résoudre les problèmes liés aux rapports
- Comprendre les concepts des playbooksCréer et surveiller les playbooks

Pré-requis:

- Familiarité avec les sujets présentés dans les cours FortiGate
- La connaissance de la syntaxe SQL SELECT est utile

Test et certification

Contenu:

- Introduction et accès initial
- Logging
- FortiSoC—Events et Incidents
- Reports
- FortiSoC—Playbooks

Méthodes pédagogiques :

Un support de cours officiel sera fourni aux participants.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement